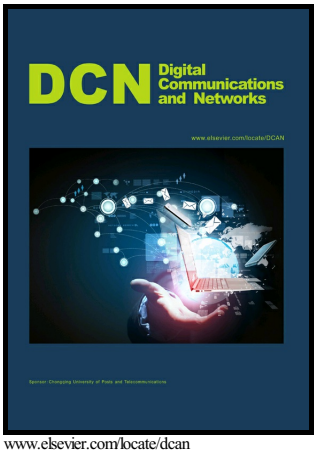

www.elsevier.com/locate/dcan

Using Discriminant Analysis to Detect Intrusions in External Communication of Self-Driving Vehicles

Khattab M Ali Alheeti, Anna Gruebler, Klaus McDonald-Maier

PII: S2352-8648(17)30091-3
DOI: http://dx.doi.org/10.1016/j.dcan.2017.03.001
Reference: DCAN77

To appear in: *Digital Communications and Networks*

Received date: 25 September 2016
Revised date: 26 February 2017
Accepted date: 7 March 2017

Cite this article as: Khattab M Ali Alheeti, Anna Gruebler and Klaus McDonald-Maier, Using Discriminant Analysis to Detect Intrusions in External Communication of Self-Driving Vehicles, *Digital Communications and Networks,* http://dx.doi.org/10.1016/j.dcan.2017.03.001

Digital Communications and Networks(DCN)

ACCEPTED MANUSCRIPT

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/dcan

Using Discriminant Analysis to Detect Intrusions in External Communication of Self-Driving Vehicles

Khattab M Ali Alheeti*, Anna Gruebler, Klaus McDonald-Maier

Embedded and Intelligent Systems Research Laboratory, School of Computer Science and Electronic Engineering, University of Essex Wivenhoe Park, Colchester CO4 3SQ, UK;
kmali@essex.ac.uk, contact@annagruebler.com (A.G.); kdm@essex.ac.uk (K.M.-M.)

Abstract

Security systems are considered a necessity for the deployment of smart vehicles in our society. Security in vehicular ad hoc networks is crucial to the reliable exchange of information and control data. In this paper, an intelligent intrusion detection system (IDS) is proposed to protect the external communication of self-driving and semi self-driving vehicles. This technology has the ability to detect Denial of Service (DoS) and black hole attacks on VANETs. The advantage of the proposed IDS over incumbent security systems is that it detects the attack before it causes significant damage. The intrusion prediction technique is based on a Linear Discriminant Analysis (LDA) and Quadratic Discriminant Analysis (QDA) to predict the attack based on an observed vehicle behaviour. Simulations utilised Network Simulator version 2 to demonstrate that the IDS exhibits a low rate of false alarms and high accuracy in detection.

KEYWORDS:
Security communication, vehicle ad hoc networks, IDS, self-driving vehicles, linear and quadratic discriminant analysis.

1. Introduction

Self-driving and semi self-driving vehicles are attracting increased attention from both industry and research community because of their potential positive and economic effects on society [1]. These vehicles depend heavily on internal and external communication systems to achieve their goals, such as traffic safety, ideal exploitation of resources, reducing human error and reducing the number of injuries and fatalities from traffic accidents [2]. In other words, autonomous and semi-autonomous vehicles operate without drivers and have the ability of improving traffic flow for vehicles on roads and reducing the number of human errors [3].

Vehicular Ad hoc Networks (VANETs) are external communication systems for these vehicles which support intelligent transportation systems [4]. VANETs an play important role in establish secure and safe environment for self-driving and semi self-driving vehicles [5]. VANETs applications can be classified into safety and non-safety applications [6]. Real-time safety applications, fleet management services, traffic management and monitoring are the most important features of these networks [7, 8]. Moreover, security systems are a very important factor for the safe application of these vehicles [7]. Strong and reliable security mechanisms are needed to protect information as well as the control data transferred between vehicles and their Road Side Units (RSUs) in radio coverage areas [8].

The IDS can be used as an effective tool to know whether unauthorized users are trying to gain access, already have access or have compromised the network. However, when IDS is compared with the wired network, there is an introduction of additional challenges in setting up an IDS by the dynamic topology of ad hoc

*Khattab M Ali Alheeti (Corresponding author) is with the School of Computer Science and Electronic Engineering, University of Essex, Colchester, CO4 3SQ, UK (e-mail: kmali@essex.ac.uk). Anna Gruebler is currently Head of Data Science at AltViz in London - Data Scientist, UK. (e-mail: contact@annagruebler.com). Klaus McDonald-Maier is with the School of Computer Science and Electronic Engineering, University of Essex, Colchester, CO4 3SQ, UK (e-mail: kdm@essex.ac.uk).

networks. Traditional security systems are sometime unable to provide a safe environment and sufficient protection for sensitive data [1]. Traditional methods can only identify external attacks and they are unable to detect and block the internal malicious vehicles. In order to detect the internal attacks, an intelligent security system is proposed that is based on behaviour and trail data. This data was collected from the trace file to monitor normal and abnormal behaviour for automobile vehicles. VANETs are a subclass/subtype of mobile ad hoc networks (MANETs) [9]. There have been some attempts to secure MANETs routing protocol. For instance, Secure Efficient Ad hoc Distance vector routing protocol (SEAD) [10], the secure on-demand routing protocol - Ariadne[11], Authenticated Routing for Ad hoc Networks (ARAN) [12], Security-Aware Ad hoc Routing (SAAR) [13], Resiliency Oriented Secure (ROS) [14], Secure Routing Protocol (SRP) [15], Secure AODV (SAODV) [16], Secure Link-State Protocol (SLSP) [17], Cooperative Security-Enforcement Routing (CSER) [18]. The above routing schemes cannot eliminate completely all of the internal (or insider) attacks even if they are implemented correctly. This is due to attackers already being inside the network with adequate credentials. For instance, a compromised mobility node has all the vital cryptographic keys and can easily launch several types of attacks, for example grey hole attacks, routing loop attacks and black hole attacks. Hence, it is also important to develop response and detection techniques for VANETs that are applicable to the above attacks. Figure 1 shows how communications take place between vehicles and RSUs in a single zone, VANETs allow mobile vehicles to communicate with other vehicles (V2V) and with infrastructures on the side road (V2R).

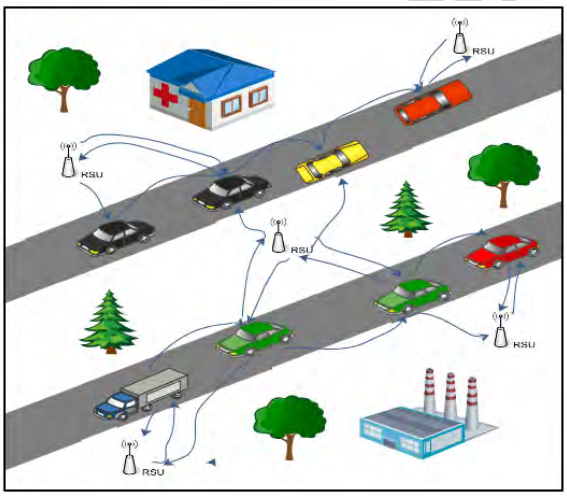

Fig. 1: VANETs Architecture

It is necessary to create an intelligent anomaly intrusion detection system (IDS) to secure the routing protocol on the network layer from potential internal and external attacks. Thus, the detection of intrusion forms thus a secondary defence. The IDS can be used as an effective tool for identifying whether unauthorised users are trying to gain access, already have access or have compromised the network. However, when IDS is compared with wired networks, there are additional challenges in setting up an intrusion detection system due to the dynamic topology of ad hoc networks. IDS has recently been utilised in the external communication of vehicles to identify and block any attacks/threats that target the communication systems. Decision for the detection frameworks is based on the current normal and abnormal behaviour of monitored self-driving vehicles [8], [19], [20]. The contributions of this paper, are summarised as follows:

- An intelligent IDS system is proposed that utilises Linear Discriminant Analysis (LDA) and Quadratic Discriminant Analysis (QDA) to detect anomalies and malicious behaviour for self-driving and semi self-driving vehicles.
- The proposed security system is not dependent on extra and expensive hardware such as Radar, Lidar and computer vision or any RSUs.

Section two a related work in the domain of security systems in ad hoc network. Section three discusses intrusion detection systems, Section four explains the simulation system and Section five describes the simulation results. Section six discusses our results. Section seven conclusion and future works.

2. Related Works

Autonomous vehicles are becoming more open and connected with the external environment. This development increases the possibility of attacks as it encourages intruders to launch different types of attacks on vehicles [6]. These vulnerabilities have direct negative effects not only on passengers, but also on pedestrians around them. The external communication system for self-driving and semi self-driving vehicles face many security problems in the wireless communication system. The IDS role is collecting traffic data from the communication system, analysing it and then identifying/blocking any malicious behaviour in the VANETs.

The wireless communication system are autonomous vehicles helps to prevent common problem such as drivers errors. In addition, VANETs supply critical data and information for emergency case, warning and notification messages. Hence, security and privacy are considered very important issue to the VANETs. Although many previous studies address problems in VANETs, but there still remain many security issues that need addressing. Studies such as Ozgur et al. have employed cognitive techniques to enhance communication performance in wireless sensor networks [21].

2.1. Packet Drop Intrusion Detection

Alheeti et al. [22] designed an intelligent intrusion detection for securing control data and information which are transferred between self-driving vehicles and the infrastructure. Malicious vehicles were blocked and detected by an IDS in a radio zone. The detection system was based on the Fuzzy Petri Nets to create sufficient protection system. In [23], Uyyala designed an anomaly detection system in secure MANETs for the black hole and grey hole attacks. It could detect and isolate the malicious behaviour of nodes. As a result, the authors improved network performance. In [24], the authors developed an anomaly detection system to secure the MANETs from the potential attacks. It was based on Fuzzy Interface System (FIS) to detect abnormal behaviour in MANETs. The IDS was capable of identifying the packet dropping attacks with high accuracy and low false positive rates. In [25], the adaptive detection threshold is utilised in design intrusion detection to identify intelligent abnormal activities in VANETs. The proposed security system can idenity immediately any malicious behaviours in VANETs that extracted from mobile vehicles. Morever, it has the ability to detect malicious behaviours with high rate of packet delivery and detection process.

2.2. Routing Protocols

Zaidi [26] presented an intrusion detection system using a statistical technique to detect a false information attack. Traffic models were used to detect rogue nodes in VANETs. The authors used different types of parameters, for instance transmission intervals with a large number of vehicles, to decide between normal and abnormal behaviour. Ali et al. designed an intrusion detection system to protect external communication of driverless and semi-driverless vehicles [27]. The proposed IDS was based heavily on the features that had been extracted from the trace file of ns-2. Support Vector Machines (SVM) and Feed-Forward Neural Networks (FFNN) were used to build an intelligent IDS that had the ability to detect and block two common types of attacks, which are: grey hole and rushing attacks.

Coussement et al. have designed security system to identify abnormal behaviours that have negative impact on theexternal communication system in mobile vehicles [28]. The proposed system required to examin income and outcome communication packets to detect attacks. It is based on decision making mechanism to secure sensitive information of VANETs. However, two approaches of security are configured the first one on vehicles whereas the second one on RSUs. These systems work together to established groups of mobile nodes based on their speed. Moreover, the proposed security systrm is based on two IDS schemes and clusterisation of mobile nodes.

2.3. Cross-layer Intrusion Detection

In [29], the authors proposed a cooperative intrusion detection to identify black hole attacks. It was based on the cross-layer architecture: MAC and network layers detection systems used the knowledge of VANETs and vehicle conditions to determine the vehicle behaviour. The cross-layer security system reduced the number of false alarm and enhanced the detection accuracy rate.

Marve et al. proposed an intrusion detection based on a cross-layer intrusion detection system to detect DoS and Distributed Denial of Service (DDoS) attacks at a different layer of the transfer protocol stack [30]. The authors were able to design a security system to provide sufficient protection for nodes in MANETs while reducing the number of false alarms.

In [31] the authors propose a cross-layer architecture in building IDS that had the ability to detect the malicious nodes and different types of DoS attacks. In addition, the proposed anomaly detection could detect different kinds of sink hole attacks and flooding attacks in an efficient way.

Akyildiz et al. proposed a novel technology to fix common problems for wireless networks which is xG networks. The proposed system had the ability to improve communication performance by increase available spectrum and improve efficiency in spectrum consumption [32].

Since autonomous technology is a relatively newer concept, more research and proposals should be done to prove its effectiveness and applicability. Security and privacy must be taken into consideration to ensure the success of self-driving and semi-self-driving vehicles. In our research, a security system is proposed to protect the external network of these vehicles from common attacks such as: DoS, black hole and grey hole attacks. It is based on the features of the trace file that have been generated from ns-2.

3. Intrusion Detection Systems (IDS) Overview

Typically, VANETs have two security layers [33]. These are suggested to protect internal and external communication systems of these vehicles in autonomous and semi-autonomous vehicles: Intrusion Prevention Systems (IPS) and IDS [34]. Security measures are now a serious topic in automotive systems since the first layer does not have the capacity to provide enough security [35].

Additionally, the external communication of these vehicles can provide a variety of services like safety and non-safety applications which aid the increasing research efforts and growing interest in security systems. IDS is seen as one of the ways of protecting VANETs, as it can detect malicious or abnormal activity on the host or network [36]. It has the capacity to delivers enough security and privacy to systems or networks since they play a vital role in identifying and

preventing internal attacks which cannot be identified or blocked by other security methods. Moreover, some studies have confirmed that IDS are effective in detecting any unauthorised access [37].

3.1. IDS Categories

IDS can be categorised in different ways; however, the major classification is: misuse, anomaly, and specifications detection systems [38]. Each detection method possesses some qualities that separate it from others, whether positive or negative. Yet, all these methods try to provide adequate security, prevent any unauthorised access, and detect all unauthorised access from malicious vehicles or nodes [38].

- Signature-based system - This type of detection technique involves a security system which contains a database of the behaviour of possible attacks. This data set can be compared to the behaviour of the system and intrusion can be detected when there is a match.
- Anomaly-based system - This detection system depends on behaviour which is already known. There is an intrusion if the system detects any deviation from this behaviour. Moreover, the system depends on a profile which is developed from the normal behaviour of the network.
- Specifications-based system - This detection system can be said to be a set of conditions whose availability in the protocol or program is necessary. The intruder can be detected when these conditions are not met.

There are many mechanisms that can be utilised in the protection of the communication system of self-driving and semi-self-driving vehicles, but we have chosen IDS because: It is designed to detect internal attacks, which is an advantage over conventional security mechanisms such as cryptographic methods which cannot detect internal attacks. In our paper, we propose intelligent IDSs which depend on the behaviours of vehicles that are collected from the trace file. The trace file is generated from the ns-2.

The proposed IDS is deployed on each vehicle that plays an important role in detecting external/internal attacks on the VANETs of self-driving and semi-self-driving vehicles without the need for additional hardware.

4. The Proposed Scheme

The intelligent proposed IDS first generates the malicious behaviour for self-driving vehicles. The network simulator requires tools to establish a realistic world of abnormal and normal behaviours for autonomous vehicles. In other words, the mobility and traffic model are generated in the early step of the proposed IDS. The overall architecture of the proposed intrusion detection system is shown in Figure 2. The security system requires a series of processing steps that are explained below.

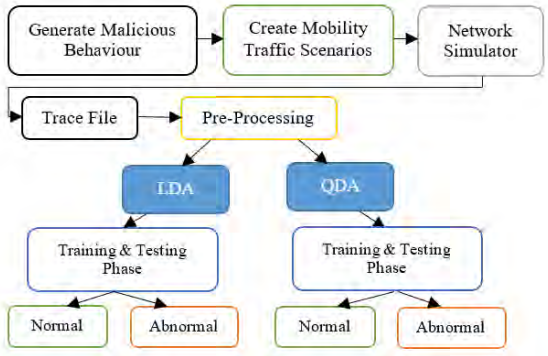

Fig. 2: VANETs Architecture

The proposed IDS is heavily based on behaviour features that have been extracted from the trace file. It is generated from the ns-2 that reflect vehicles behaviour wheather normal or malicious. The extracted features require pre-processing phase to prepare it to the training phase for LDA and QDA such as encoding, normalisation and uniform distribution. In this case, the extracted dataset is ready to train and test phases for LDA and QDA.

4.1. Establish Abnormal Behaviour

Here, a malicious vehicle behaviour is added in ns-2 utilising the VANETs - Ad hoc On-Demand Distance Vector Routing (AODV) routing protocol. In this security system, new routing protocol which is VANETs - AODV that is utilised to evaluate the performance of the proposed IDS. The generated behaviour of a mobility node is called a DoS vehicle when it makes network resources unavailable to rightful users in the VANETs.

In order to generate DoS behaviour in VANETs, we need to modify and reformulate some internal parameters of the two files in the routing protocol. In other words, two files of AODV-VANETs are needed to modify and establish the malicious behaviour which are: VANETs - AODV.cc and VANETs - AODV.h. In addition, the TCL scenario for VANETs requires to add a few lines of code for simulating this behaviour under certain condition such as: ns-2 at specific time [vehicle number n set DoS]. The malicious vehicle is an abnormal entity which will drop the router packets. In addition, the malicious scenario needs updating and changing to some functions in the TCL program to run DoS functions that were established in VANETs - AODV files.

4.2. Create Mobility and Traffic Scenarios

In this research, ns-2 is employed to evaluate the overall performance of the proposed system and to calculate the amount of false alarms generated from

it. ns-2 requires software to generate a realistic environment of malicious and normal behaviours for self-driving vehicles by providing two types of inputs traffic and mobility scenarios which are: Simulation of Urban Mobility Model (SUMO) and MObilty VEhicles (MOVE) [39]-[40]. These tools allow ns-2 simulate successfully the external communications of these vehicles within the different scenarios.

SUMO is considered an efficient mobility program that has been used in generating a real environment in VANETs [41]. In addition, SUMO provides efficient computation even with city and downtown scenarios, i.e. with large number of vehicles [41]. MOVE is based on SUMO [41]. It obtains the output file generated in SUMO by converting them to ns-2. Bushra et al. presented a comprehensive survey of wireless communication in urban areas. The authors classify all urban application scenarios that were employed in desgin mobility system in urban area [42]. The Manhattan urban mobility model is utilised in designing the mobility and traffic scenario for self-driving vehicles, which is widely adopted in scientific research [43]. Figure 3 below presents the traffic and mobility scenario for driverless vehicles.

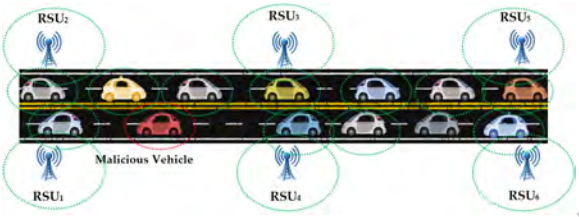

Fig. 3: Traffic and Mobility Scenario

The mobility and traffic model of the self-driving and semi-autonomous vehicles is shown in figure 3. It describes the communication between vehicles and with RSUs in that radio coverage area. The Manhattan mobility model is utilised in design for some reasons, such as flexibility and common used in VANETs.

4.3. Features from the Trace File

The trace file describes all events and actions of vehicles communication in VANET. In contrast, the proposed security system is based on the features which have been extracted from the trace file [44]. The proposed security system is based on the features extracted from the trace file of the ns-2. In general, the trace file is divided into three subset files which are: basic trace, internet protocol trace and VANETs - AODV trace [41]. However, the performance and efficiency of the detection system depend heavily on the type and number of the extracted features. To evaluate the efficiency of the detection system, we used all the 21 features of the trace file that reflect behaviour of a mobility node on the street [1].

The proposed IDS are based on Linear Discriminant Analysis (LDA) and Quadratic Discriminant Analysis (QDA) which have the ability to learn normal and malicious behaviour through the training phase. Ultimately reducing the cost and enhancing real-time detection are considered a main motivation for utilizing the artificial intelligence in building intelligent IDS [45].

4.4. Linear and Quadratic Discriminant Analysis

Discriminant methods, whether linear or quadratic, are efficiently and mathematically robust and they often create classification systems whose precision is as good as more complex methods [46]. The work principle of an LDA is based on Bayes optimal classifier and a linear separating hyper plane is employed in basic classification between classes in LDA [47]. Equation 1 shows the linear discriminant function [47]:

$$d_k(\chi) = 2\mu_k^T \sum_{k}^{1-} \chi - \mu_k^{-1}\mu_k - 2\log\pi(k) \tag{1}$$

where: k representes normal and abnormal classes, π_k is prior probability, χ is set of measurements, $\sum_k$ is convariance matrix and μ_k is mean vector. The QDA is considered a generalised version of LDA and it can discriminate only two classes of points [48]. The discriminant function of LDA is used for the QDA after multiplied by -2 as shown in Equation 2 [49]:

$$d_k(\chi) = (\chi - \mu_k)^T \sum_k^{-1} (\chi - \mu_k) + \log|\sum_k| - 2\log\pi_k \tag{2}$$

The discriminant rule of QDA is shown in Equation 3 [50]:

$$d_k(\chi) = \min_{1\le k\le k} d_k(\chi) \Leftrightarrow \max_{1\le k\le k} p^{(\chi/k)} \tag{3}$$

where, $p^{(\chi/k)}$ posterior distribution. The training and testing phases are applied on the experimental section.

4.5. Fuzzification of the Data

The extracted features have direct impact on the performance of the proposed security system. In other words, the number and type of features play vital role on the detection rate and the number of false alarms. The dataset of security system suffers from common classification problems such as, the normal and malicious vehicles is not obvious from the extracted features, or they do not draws clear line border between normal and abnormal. In this case, the optimal solution is fuzzification model on extracted dataset from ns-2. In this paper, a mathematical model is designed to redistribute the features and cope with ambiguity.

However, the mathematical model is proposed to address the classification problem [51]. In the previous study, security system is designed without fuzzification model and we got a false alarm rate of 12.24 but after incorporating fuzzifcation we obtain 0.17

[52]. Each feature value was distributed in five values in equation 4 with a range in [0.1] which are: low, medium low, medium, medium high and high.

$$f(x, a, b, c) = \max(\min((x - a)/(b - a), (c - x)/(c - b)), 0) \quad (4)$$

where x is the feature value while a, b and c represent the values of the fuzzy domain. The fuzzifcation IDS can increase the detection rate of the proposed IDS while reducing the number of false alarms at the same time.

4.6. Network Simulator Parameters and Environment

In this paper, the communication system of self-driving vehicles is built on the ns-2. The network simulator is designed to simulate wired and wireless networks [39]. However, the designers faced problems in simulating the external communications of self-driving vehicles with ns-2. A major reason for this is that the basic ns-2 simulator has not been designed to support the simulation of VANETS. It was problematic for the designers to simulate the VANETS of self-driving with ns-2 because of the unavailability of ns-2. In this case, extra tools are employed with ns-2 for simulating VANETs for self-driving and semi-self-driving vehicles. These software are SUMO and MOVE [53]. The ns-2, traffic and mobility systems are utilised to achieve the intelligent intrusion detection system for the external communication system in the real world. In this proposal, the communication environment is compsed of 30 cars and six RSUs [39].

4.7. The Proposed Intelligent Detection System

The proposed security system is utilised by/in LDA and QDA to protect the external communication system for self-driving and semi self-driving vehicles. It has the ability to distinguish between normal and malicious communication between vehicles and RSUs. The proposed IDS has six stages as following:

- Stage I (Generate the traffic and the mobility model): At this stage, SUMO and MOVE are employed to generate the suitable scenarios for ns-2. The SUMO and MOVE output files are considered input files for the next step.
- Stage II (network simulator): The behaviour for vehicles whether normal or abnormal is generated to simulate vehicles. Two output files are obtained at this stage which are trace and Network Animator (NAM) files. The features are extracted from the trace file that has been generated from the ns-2.
- Stage III (Data collection and pre-processing): At this stage, the trace file is utilised to extracted communication features for vehicles. In addition, the extracted features are pre-processed by transforming them to numeric values and the values were normalized to values betweenn 0 and 1 according to the equation 5:

$$X = \frac{X - min}{max - min} \quad (5)$$

Normalising data often permits to enhance the performance of LDA and QDA as well as increasing detection rate.

- Stage IV (Fuzzification): The fuzzy set is employed to convert the extracted features to their fuzzified counterparts to fix classification problem and dataset overlap.
- Stage V (Training phase): LDA and QDA are trained with the extracted dataset. The raw dataset is divided into six subsets, each subset containing ten thousand records. For each iteration of the training cycle, the proposed system is used a different subset in this phase.
- Stage VI (Testing phase): At this stage, the proposed IDS is tested with different subset to calculate the detection rate and number of false alarms. The testing phase has the ability to calculate performance metrics for this system.

5. Expermental Results

In this paper, the detection system can identify normal or abnormal/malicious behaviour through the proposed security system. We need real data that reflects behaviour whether normal or abnormal between vehicles and their RSUs, to evaluate performance of the proposed IDS. To obtain real data, we need to generate two kinds of scenarios and simulate these under certain conditions. This raw data is generated from the trace file that was generated from the ns-2. These features describe the normal and abnormal behaviours of self-driving and semi self-driving vehicles.The initial parameters used in this proposal could be essential part in ns-2. In other words, the behaviour and performance in ns-2 are heavily based on these parameters. Table 1 lists the parameters are utilised in this security system.

Table 1: Simulator Environment and Parameters

Parameter	Value
Simulator	ns-2.35
Simulation time	250*s*
Number of nodes	30 Vehicles
Number of RSUs	6 RSUs
Type of Traffic	Constant Bit Rate (CBR)
Topology	600 x 400 (*m*)
Transport Protocol	UDP
Packet Size	512
Routing Protocol	VANETs - AODV
Channel type	Wireless
Queue Length	50 packets
Number of Road Lanes	2
Radio Propagation Model	Two Ray Ground
MAC protocol	IEEE 802.11p
Speed	50 m/s
Interface queue type	Priority Queue
Network Interface type	Physical Wireless
Mobility Models	Manhattan Mobility Model

5.1. Performance Metrics

To measure the efficiency and the effectiveness of the proposed IDS, we need to calculate some performance metrics. They are mainly divided into three classes [54], namely:

- Ranking metric: In this metric, we calculate four types of alarms which are: True Positive *TP*, False Positive *FPk*, True Negative *TN* and False Negative *FN*. Moreover, Precision Rate *PR* and Detection Rate *DR* are calculated in this type of the metric. The accuracy of the system result is be calculated as follows [27]:

$$Accuracy = \frac{Numberofcorrectlyclassifiedpatterns}{Totalnumberofpatterns} \quad (6)$$

In addition, the measures will be calculated as follows [55]: Let *TP*=normal connection record classified as normal *TN*=attack connection record classified as attack *FP*=normal connection record classified as attack *FN*=attack connection record classified as normal: then

$$TP_{Rate(sensitivty)} = \frac{TP}{TP + FN} \quad (7)$$

$$TN_{Rate(specificity)} = \frac{TN}{TN + FP} \quad (8)$$

$$FN_{Rate} = (1 - sensitivty) = \frac{FN}{FN + TP} \quad (9)$$

$$FP_{Rate} = (1 - specificity) = \frac{FP}{FP + TN} \quad (10)$$

$$DR = \frac{Correctlydetectedattacks}{Totalnumberofattacks} \quad (11)$$

$$DR = \frac{TP + TN}{TP + TN + FP + FN}$$

$$PR = \frac{TP}{TP + FP} \quad (12)$$

- Threshold metric: Classification Rate *CR* and F-Measure *FM* are calculated in these metrics. The *FM* value lies in the range from 0 to 1. It is used to give threshold as well as it is the mean of the *PR* and Recall. In addition, Recall metric is the missing part of the *PR*. In other words, it is equivalent to the *DR*.

$$CR = \frac{Correctlyclassifiedinstances}{Totalnumberofinstances} \quad (13)$$

$$CR = \frac{TP}{TP + FN}$$

$$FM = \frac{2}{\frac{1}{PR} + \frac{1}{Recall}} \quad (14)$$

- Probability metric: Calculating Root Mean Square Error *RMSE*. The best way to explain classification results is a confusion matrix, by evaluating the performance of the proposed intelligent IDS [27].
- Packet Delivery Rate (PDR): The PDR value is ratio between send packets from source vehicle and received packets at destination vehicle.

$$PDR = \frac{\sum Numberofpacketsreceived}{\sum NumberofpacketsSent} \quad (15)$$

- Throughput: The total number of packets which exchanged in the VANETs. It is utilised to measure the effectiveness of the routing protocol.

$$Throughput = \frac{Numberofreceived*packetssize}{SimulationTime} \quad (16)$$

- End-to-end Delay:It is based on time to calculated the average packet delay. In other words, this metric is the average time to reach the secnd packets from the source node to the destination node.

$$End-to-endDelay = \frac{\sum EndTime-StartTime}{\sum Numberofconnections} \quad (17)$$

5.2. Training and Testing LDA-IDS and QDA-IDS to detect Malicious Behaviour

The extracted features are utilised in the training and testing phase for the proposed anomaly detection system. We have used a 100-fold cross-validation to decrease the bias related to the random splitting of the data set into training phase and testing phase. The security system must be able to detect novel and existing attacks. The obtained classification rate for LDA and QDA, time and error rate are as shown in Table 2:

Table 2: Classification Rate

IDS			
Class	Accuracy – Test Phase	Time/s	Error Rate-Train Phase
LDA-Normal	99.94%	8.79s	0.385
LDA-Abnormal	81.09%		
Class	Accuracy– Test Phase	Time/s	Error Rate-Train Phase
QDA-Normal	91.07%	14.27s	0.397
QDA-Abnormal	78.87%		

In Table 3, we determine four types of alarms: *TP, FP, TN and FN* for the proposed security system.

Table 3: Alarm Rate

Alarm Type	LDA	QDA
True positive	86.44%	84.55%
True negative	92.73%	87.44%
False positive	7.27%	12.56%
False negative	13.56%	15.45%

In addition, we need to determine some extra performance metrics for each of the proposed IDS which are LDA-IDS and QDA-IDS for evaluation of their performance individually. The Classification Rate *CR*, Detection Rate *DR*, Precision Rate *PR*, F-Measure *FM*, *P-value* and mean error are calculated in Table 4.

Table 4: Performance Metrics

Performance Metrics						
Class	CR	DR	PR	FM	P-value	Mean Error
LDA	88.87%	86.44%	94.99%	0.9	8.7E-08	0.385%
QDA	84.55%	85.67%	91.07%	0.88		0.397%

The *P-value* is calculated to measure the difference rate between the LDA and QDA as shown in Table 4. This value indicates that there is a significant difference between the error of the two methods.

The Packet Delivery Rate (PDR) and End-to-end delay are explained in table 5. It is easily observe the security system in providing safety and security environment of VANETs.

Table 5: Comparison Performance

Performance Metrics	VANETs without IDS	VANETs with IDS
Packet Delivery Ratio	43.59	96.67
Average End-to-End Delay	1.5442ms	1.4835ms
Average Throughput	34.21kbps	81.47kbps

6. Discussion

The motivation behind this paper is to design an intelligent IDS that provides a secure environment for autonomous and semi-autonomous vehicles. The IDS has the ability to detect abnormal behaviour and take actions to prevent attacks on the network, vehicle and the passengers. In the absence of this IDS, the security of the system cannot be certified. The proposed security system was implemented in eight phases: generating the mobility and traffic model, the ns-2, the trace file, data collection and pre-processing, training and testing for the LDA, training and testing for the QDA and comparing the performance of the two types of proposed intelligent security system.

In order to evaluate the performance detection for the proposed security system, we need to compare our proposed IDS with the previous work that achieved error rate, of 2.05 [1], 10 [28] and 19 [25], whereas in the security system presented here, we can get a 0.58 error detection rate. The average of false alarm that was generated in [1] is 12.24, while we have achieved 9.91 with this security system. Figure 4 shows the performance comparsion between our proposed security system with the previous work.

Figure 4 shows the comparison of performance between the LDA and QDA. The error rate for the LDA-IDS was 0.385. In this paper, the *TP* and *TN* alarms rate fluctuated between 86.44 and 92.73 with excellent and efficient accuracy. On the other hand, the *FN* alarm rate was accepted at about 7.27 which is a good indicator of the design results.

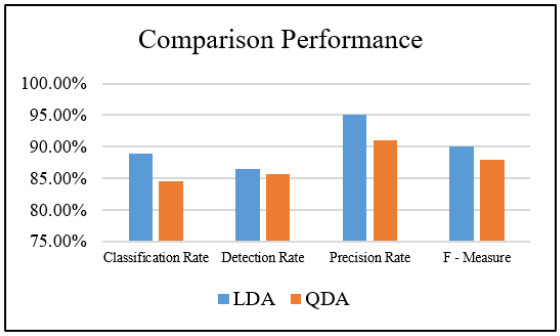

Fig. 4: performance compare between LDA and QDA

The error rate for the QDA-IDS was 0.397. The *TP* and *TN* alarms rate fluctuated between 84.55 and 87.44 with efficient accuracy. On the other hand, the *FN* alarm rate was somewhat high at about 12.56 which is an accepted indicator of the design results. We could enhance the detection rate for the proposed security system by using LDA and QDA that creates flexibility in selecting the security system that is more efficient with different conditions.

According to the experimental results section, we can easily observe that the LDA-IDS is more efficient and effective in the detection of abnormal behaviour for vehicles with a low false negative alarm rate than QDA-IDS.

7. Conclusion and Future Work

In this paper, we have proposed a reliable IDS to detect the malicious behaviour in the communication system for the self-driving and semi self-driving vehicles. The proposed IDS can detect abnormal behaviour and take actions to prevent an attack on the network, vehicle and the passengers. It is considered a prediction scheme to secure the external communication system for autonomous systems. The proposed LDA-IDS has the ability to distinguish and identify the actions of a malignant vehicle. It is considered a novel protection system to secure the external communication system because this is the first work that has employed abnormal behaviour prediction for securing VANETs.

Our proposed IDS can identify and block DoS and black hole attacks by monitoring the routing table and analysis of the trace file that has been generated from ns-2. The generated trace file defines the behaviours of the VANETs through the data control and information that were sent, received, forwarded and dropped in packets. Meanwhile, QDA has a higher error rate than LDA. Thus, we demonstrate that a simpler algorithm - LDA may yield better performance than a more complicated algorithm - QDA. The LDA and QDA make the proposed IDS more efficient in securing VANETs.

A possible further extension of the security system is to enhance RSUs with intelligent IDS and vehicles with AI techniques such as k-Nearest Neighbors algorithm (kNN).

Acknowledgements

This research has been supported by the Engineering and Physical Sciences Research Council(EPSRC) Grant EP/K004638/1 (project named RoBoSAS).

References

[1] K. M. A. Alheeti, A. Gruebler, K. D. McDonald-Maier, An intrusion detection system against malicious attacks on the communication network of driverless cars, in: 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), IEEE, 2015, pp. 916–921.

[2] M. O. Cherif, Optimization of v2v and v2i communications in an operated vehicular network, France (2010) PhD thesis.

[3] Y. Saleem, M. H. Rehmani, S. Zeadally, Integration of cognitive radio technology with unmanned aerial vehicles: issues, opportunities, and future research challenges, Journal of Network and Computer Applications 50 (2015) 15–31.

[4] M. O. Cherif, S.-M. Senouci, B. Ducourthial, Efficient data dissemination in cooperative vehicular networks, Wireless Communications and Mobile Computing 13 (12) (2013) 1150–1160.

[5] T. Umer, M. Amjad, N. Shah, Z. Ding, Modeling vehicles mobility for connectivity analysis in vanet, in: Intelligent Transportation Systems, Springer, 2016, pp. 221–239.

[6] H. Sedjelmaci, T. Bouali, S. M. Senouci, Detection and prevention from misbehaving intruders in vehicular networks, in: 2014 IEEE Global Communications Conference, IEEE, 2014, pp. 39–44.

[7] H. Sedjelmaci, S. M. Senouci, A new intrusion detection framework for vehicular networks, in: 2014 IEEE International Conference on Communications (ICC), IEEE, 2014, pp. 538–543.

[8] H. Sedjelmaci, S. M. Senouci, M. Feham, An efficient intrusion detection framework in cluster-based wireless sensor networks, Security and Communication Networks 6 (10) (2013) 1211–1224.

[9] S. Yousefi, M. S. Mousavi, M. Fathy, Vehicular ad hoc networks (vanets): challenges and perspectives, in: 2006 6th International Conference on ITS Telecommunications, IEEE, 2006, pp. 761–766.

[10] Y.-C. Hu, D. B. Johnson, A. Perrig, Sead: Secure efficient distance vector routing for mobile wireless ad hoc networks, Ad hoc networks 1 (1) (2003) 175–192.

[11] Y.-C. Hu, A. Perrig, D. B. Johnson, Ariadne: A secure on-demand routing protocol for ad hoc networks, Wireless networks 11 (1-2) (2005) 21–38.

[12] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, E. M. Belding-Royer, A secure routing protocol for ad hoc networks, in: Network Protocols, 2002. Proceedings. 10th IEEE International Conference on, IEEE, 2002, pp. 78–87.

[13] S. Yi, P. Naldurg, R. Kravets, Security-aware ad hoc routing for wireless networks, in: Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing, ACM, 2001, pp. 299–302.

[14] A. A. Pirzada, C. McDonald, Secure routing protocols for mobile ad hoc wireless networks, Advanced Wired and Wireless Networks.

[15] P. Papadimitratos, Z. J. Haas, Secure routing for mobile ad hoc networks, in: the SCS Commnication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), San Antonio, TX, January 27-31, 2002, 2002, pp. 193–204.

[16] M. G. Zapata, Secure ad hoc on-demand distance vector routing, ACM SIGMOBILE Mobile Computing and Communications Review 6 (3) (2002) 106–107.

[17] P. Papadimitratos, Z. J. Haas, Secure link state routing for mobile ad hoc networks, in: Applications and the Internet Workshops, 2003. Proceedings. 2003 Symposium on, IEEE, 2003, pp. 379–383.

[18] B. Lu, U. W. Pooch, Cooperative security-enforcement routing in mobile ad hoc networks, in: Mobile and Wireless Communications Network, 2002. 4th International Workshop on, IEEE, 2002, pp. 157–161.

[19] S. S. Doumit, D. P. Agrawal, Self-organized criticality and stochastic learning based intrusion detection system for wireless sensor networks, in: Military Communications Conference, 2003. MILCOM'03. 2003 IEEE, Vol. 1, IEEE, 2003, pp. 609–614.

[20] S. Shin, T. Kwon, G.-Y. Jo, Y. Park, H. Rhy, An experimental study of hierarchical intrusion detection for wireless industrial sensor networks, IEEE Transactions on Industrial Informatics 6 (4) (2010) 744–757.

[21] O. B. Akan, O. B. Karli, O. Ergul, Cognitive radio sensor networks, IEEE network 23 (4) (2009) 34–40.

[22] K. M. A. Alheeti, A. Gruebler, K. D. McDonald-Maier, A. Fernando, Prediction of dos attacks in external communication for self-driving vehicles using a fuzzy petri net model, in: 2016 IEEE International Conference on Consumer Electronics (ICCE), IEEE, 2016, pp. 502–503.

[23] A. Mitrokotsa, R. Mavropodi, C. Douligeris, Intrusion detection of packet dropping attacks in mobile ad hoc networks, in: Proceedings of the International Conference on Intelligent Systems And Computing: Theory And Applications, 2006, pp. 111–118.

[24] A. Chaudhary, V. Tiwari, A. Kumar, Design an anomaly based fuzzy intrusion detection system for packet dropping attack in mobile ad hoc networks, in: Advance Computing Conference (IACC), 2014 IEEE International, IEEE, 2014, pp. 256–261.

[25] C. A. Kerrache, A. Lakas, N. Lagraa, Detection of intelligent malicious and selfish nodes in vanet using threshold adaptive control, in: Electronic Devices, Systems and Applications (ICEDSA), 2016 5th International Conference on, IEEE, 2016, pp. 1–4.

[26] K. Zaidi, M. Milojevic, V. Rakocevic, A. Nallanathan, M. Rajarajan, Host based intrusion detection for vanets: A statistical approach to rogue node detection.

[27] K. M. A. Alheeti, A. Gruebler, K. D. McDonald-Maier, On the detection of grey hole and rushing attacks in self-driving vehicular networks, in: Computer Science and Electronic Engineering Conference (CEEC), 2015 7th, IEEE, 2015, pp. 231–236.

[28] R. Coussement, B. Amar Bensaber, I. Biskri, Decision support protocol for intrusion detection in vanets, in: Proceedings of the third ACM international symposium on Design and analysis of intelligent vehicular networks and applications, ACM, 2013, pp. 31–38.

[29] R. Baiad, H. Otrok, S. Muhaidat, J. Bentahar, Cooperative cross layer detection for blackhole attack in vanet-olsr, in: 2014 International Wireless Communications and Mobile Computing Conference (IWCMC), IEEE, 2014, pp. 863–868.

[30] T. K. Marve, N. U. Sambhe, A review on cross layer intrusion detection system in wireless ad hoc network, in: Electrical, Computer and Communication Technologies (ICECCT), 2015 IEEE International Conference on, IEEE, 2015, pp. 1–4.

[31] R. Shrestha, K.-H. Han, D.-Y. Choi, S.-J. Han, A novel cross layer intrusion detection system in manet, in: 2010 24th IEEE International Conference on Advanced Information Networking and Applications, IEEE, 2010, pp. 647–654.

[32] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, S. Mohanty, Next generation/dynamic spectrum access/cognitive radio wireless networks: a survey, Computer networks 50 (13) (2006) 2127–2159.

[33] R. H. S. driving Car Sensors, Researcher hacks self-driving car sensors, http://spectrum.ieee.org/cars-that-think/transportation/self-driving/researcher-hacks-selfdriving-car-sensors (March 2015).

[34] G. Samara, W. A. Al-Salihy, R. Sures, Security issues and challenges of vehicular ad hoc networks (vanet), in: New Trends in Information Science and Service Science (NISS), 2010 4th International Conference on, IEEE, 2010, pp. 393–398.

[35] M. N. Mejri, J. Ben-Othman, M. Hamdi, Survey on vanet security challenges and possible cryptographic solutions, Vehicular Communications 1 (2) (2014) 53–66.

[36] D. Tian, Y. Wang, G. Lu, G. Yu, A vehicular ad hoc networks intrusion detection system based on busnet, in: Future Computer and Communication (ICFCC), 2010 2nd International Conference on, Vol. 1, IEEE, 2010, pp. V1–225.

[37] R. Bronte, H. Shahriar, H. M. Haddad, A signature-based intrusion detection system for web applications based on genetic algorithm, in: Proceedings of the 9th International Conference on Security of Information and Networks, ACM, 2016, pp. 32–39.

[38] Y. Ping, J. Xinghao, W. Yue, L. Ning, Distributed intrusion detection for mobile ad hoc networks, Journal of systems engineering and electronics 19 (4) (2008) 851–859.

[39] T. N. S. ns 2, The network simulator - ns-2, www.isi.edu/nsnam/ns (June 2014).

[40] J. Harri, F. Filali, C. Bonnet, Mobility models for vehicular ad hoc networks: a survey and taxonomy, IEEE Communications Surveys & Tutorials 11 (4) (2009) 19–41.

[41] C. . C. C. Consortium, Car 2 car communication consortium, www.car-2-car.org/index.php?id=5 (June 2011).

[42] B. Rashid, M. H. Rehmani, Applications of wireless sensor networks for urban areas: a survey, Journal of Network and Computer Applications 60 (2016) 192–219.

[43] J. Breu, A. Brakemeier, M. Menth, Analysis of cooperative awareness message rates in vanets, in: ITS Telecommunications (ITST), 2013 13th International Conference on, IEEE, 2013, pp. 8–13.

[44] S. Chettibi, Y. Labeni, A. Boulkour, Trace file analyzer for ad hoc routing protocols simulation with ns2, in: New Technologies of Information and Communication (NTIC), 2015 First International Conference on, IEEE, 2015, pp. 1–6.

[45] Using artificial intelligence to create a low cost self-driving car, http://budisteanu.net/Download/ISEF 20220Autonomous20car20 Doc20particle.pdf (Jule 2015).

[46] T. Rasymas, V. Rudžionis, Evaluation of methods to combine different speech recognizers, in: Computer Science and Information Systems (FedCSIS), 2015 Federated Conference on, IEEE, 2015, pp. 1043–1047.

[47] D. S., Statistical data mining and machine learning, Tech. rep., Department of Statistics Oxford (2016).

[48] S. Bhattacharyya, A. Khasnobish, S. Chatterjee, A. Konar, D. Tibarewala, Performance analysis of lda, qda and knn algorithms in left-right limb movement classification from eeg data, in: Systems in Medicine and Biology (ICSMB), 2010 International Conference on, IEEE, 2010, pp. 126–131.

[49] S. H. Baek, D.-H. Park, H. Bozdogan, Hybrid kernel density estimation for discriminant analysis with information complexity and genetic algorithm, Knowledge-Based Systems 99 (2016) 79–91.

[50] J. H. Friedman, Regularized discriminant analysis, Journal of the American statistical association 84 (405) (1989) 165–175.

[51] G. Chen, T. T. Pham, Introduction to fuzzy sets, fuzzy logic, and fuzzy control systems, CRC press, 2000.

[52] K. M. A. Alheeti, A. Gruebler, K. D. McDonald-Maier, An intrusion detection system against black hole attacks on the communication network of self-driving cars, in: 2015 Sixth International Conference on Emerging Security Technologies (EST), IEEE, 2015, pp. 86–91.

[53] K.-c. Lan, C.-M. Chou, Realistic mobility models for vehicular ad hoc network (vanet) simulations, in: ITS Telecommunications, 2008. ITST 2008. 8th International Conference on, IEEE, 2008, pp. 362–366.

[54] R. Caruana, A. Niculescu-Mizil, Data mining in metric space: an empirical analysis of supervised learning performance criteria, in: Proceedings of the tenth ACM SIGKDD international conference on Knowledge discovery and data mining, ACM, 2004, pp. 69–78.

[55] G. Creech, J. Hu, A semantic approach to host-based intrusion detection systems using contiguousand discontiguous system call patterns, IEEE Transactions on Computers 63 (4) (2014) 807–819.